Notice of Allowability	Application No.	Applicant(s)	
	09/553,415	OBANA, SATOSHI	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *RCE filed on 4/07/2005*.

2. ☒ The allowed claim(s) is/are *1-63*.

3. ☒ The drawings filed on *20 April 2000* are accepted by the Examiner.

4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *06/09/2005* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Phillip Articola (Registration No. 38,819) on June 9, 2005.

The application has been amended as follows:

Examiner's Amendments to the Claims:

Claim 1 (only first limitation is amended from Applicant's submitted claims)

1. An encrypting apparatus comprising:

an encrypting operation section carrying out an encrypting operation to a plaintext using intermediate data at each of the plurality of encrypting stages of said encrypting operation to produce a ciphertext, wherein said encrypting operation section outputs encrypting stage data indicating an encrypting state at each of said plurality of encrypting stages;

a determining section determining whether said encrypting operation at a next encrypting stage should be changed, based on said encrypting stage data at a current encrypting stage from said encrypting operation section;

a control section changing said encrypting operation at said next encrypting stage a plurality of times when it is determined that said encrypting operation at said next encrypting stage should be changed,

wherein said determining section determines whether said intermediate data at said next encrypting stage of said encrypting operation should be changed depending on at least a plurality of random numbers, based on said encrypting stage data at said current encrypting stage from said encrypting operation section,

wherein said encrypting stage data includes said intermediate data at said next encrypting stage, and

wherein said control section changes said intermediate data at said next encrypting stage a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said encrypting operation,

wherein said encrypting operation section divides each n-bit word of the plaintext into an upper n bits and a lower n bits, n being an even integer value greater than or equal to 16,

wherein said determining section calculates a logical product of the upper n bits of the plaintext with at least one of said plurality of random numbers to obtain a first result, and said determining section calculates a logical product of the lower n bits of the plaintext with at least one of said plurality of random numbers to obtain a second result,

wherein, in obtaining the first result and the second result, a first subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with a first of said

plurality of random numbers; a second subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with a second of said plurality of random numbers, and a third subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with both the first and second random numbers.

Claim 29 (only first limitation amended from Applicant's submitted claims)

29. A decrypting method comprising:

(a) determining whether a decrypting operation at a current decrypting stage should be changed, based on decrypting stage data at a previous decrypting stage, said decrypting stage data at said previous decrypting stage indicating an decrypting state at each of said plurality of decrypting stages;

(b) changing said decrypting operation at said current decrypting stage when it is determined that said decrypting operation at said next decrypting stage should be changed;

(c) carrying out said decrypting operation at said current decrypting stage a plurality of times to a ciphertext using intermediate data at said current decrypting stage; and

(d) executing said steps (a) to (c) to each of a plurality of decrypting stages to produce a plaintext,

wherein step (b) determines whether said intermediate data at said next decrypting stage of said decrypting operation should be changed depending on at least

a plurality of random numbers, based on said decrypting data at said current decrypting stage from said step (c),

wherein said decrypting stage data includes said intermediate data at said next encrypting stage, and

wherein, in said step (c), said intermediate data at said next decrypting stage is changed a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said decrypting operation (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10),

wherein said decrypting operation is carried out by:

i) dividing each n-bit word of the plaintext into an upper n bits and a lower n bits, n being an even integer value greater than or equal to 16,

ii) calculating a logical product of the upper n bits of the plaintext with at least one of said plurality of random numbers to obtain a first result, and

iii) calculating a logical product of the lower n bits of the plaintext with at least one of said plurality of random numbers to obtain a second result,

wherein, in obtaining the first result and the second result, a first subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with a first of said plurality of random numbers, a second subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with a second of said plurality of random numbers, and a third subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with both the first and second random numbers.

Claim 43 (Only the preamble is amended from Applicant's submitted claims)

43. A recording medium which stores a program for an encrypting method, wherein said encrypting method comprises:

(a) determining whether an encrypting operation at a current encrypting stage should be changed, based on encrypting stage data at a previous encrypting stage, said encrypting stage data at said previous encrypting stage indicating an encrypting state at said previous encrypting stage;

(b) changing said encrypting operation at said current encrypting stage when it is determined that said encrypting operation at said current encrypting stage should be changed;

(c) carrying out said encrypting operation at said current encrypting stage a plurality of times to a plaintext using intermediate data at said current encrypting stage; and

(d) executing said steps (a) to (c) to each of a plurality of said encrypting stages of said encrypting operation to produce a ciphertext,

wherein step (b) determines whether said intermediate data at said next encrypting stage of said encrypting operation should be changed depending on at least a plurality of random numbers, based on said encrypting data at said current encrypting stage from said step (c),

wherein said encrypting stage data includes said intermediate data at said next encrypting stage, and

wherein, in said step (c), said intermediate data at said next encrypting stage is changed a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said encrypting operation,

wherein said encrypting operation is carried out by:

i) dividing each n-bit word of the plaintext into an upper n bits and a lower n bits, n being an even integer value greater than or equal to 16,

ii) calculating a logical product of the upper n bits of the plaintext with at least one of said plurality of random numbers to obtain a first result, and

iii) calculating a logical product of the lower n bits of the plaintext with at least one of said plurality of random numbers to obtain a second result,

wherein, in obtaining the first result and the second result, a first subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with a first of said plurality of random numbers, a second subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with a second of said plurality of random numbers, and a third subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with both the first and second random numbers.

Claim 50 (only first limitation amended from Applicant's submitted claims)

50. A recording medium which stores a program for a decrypting method, wherein said decrypting method comprises:

(a) determining whether a decrypting operation at a current decrypting stage should be changed, based on decrypting stage data at a previous decrypting stage, said decrypting stage data at said previous decrypting stage indicating an decrypting state at each of said plurality of decrypting stages;

(b) changing said decrypting operation at said current decrypting stage when it is determined that said decrypting operation at said next decrypting stage should be changed;

(c) carrying out said decrypting operation at said current decrypting stage to a ciphertext using intermediate data at said current decrypting stage; and

(d) executing said steps (a) to (c) to each of a plurality of decrypting stages to produce a plaintext,

wherein step (b) determines whether said intermediate data at said next encrypting stage of said encrypting operation should be changed depending on at least a plurality of random numbers, based on said encrypting data at said current encrypting stage from said step (c),

wherein said decrypting stage data includes said intermediate data at said next decrypting stage, and

wherein, in said step (c), said intermediate data at said next decrypting stage is changed a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said decrypting operation,

wherein said decrypting operation is carried out by:

i) dividing each n-bit word of the plaintext into an upper n bits and a lower n bits, n being an even integer value greater than or equal to 16,

ii) calculating a logical product of the upper n bits of the plaintext with at least one of said plurality of random numbers to obtain a first result, and

iii) calculating a logical product of the lower n bits of the plaintext with at least one of said plurality of random numbers to obtain a second result,

wherein, in obtaining the first result and the second result, a first subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with a first of said plurality of random numbers, a second subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with a second of said plurality of random numbers, and a third subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with both the first and second random numbers.

Claim 57 (Only the preamble is amended from Applicant's submitted claims)

57. A recording medium which stores a program for an encrypting and decrypting method, wherein said encrypting and decrypting method comprises:

(a) determining whether an inputted instruction is an encrypt instruction or a decrypt instruction (Figure 2, Figure 12, column 2 lines 27-65, column 5 lines 1-37, column 6 lines 1-65, column 9 lines 24-58);

(b) determining whether said encrypting operation to a text at a current encrypting stage of an encrypting operation should be changed, based on said encrypting stage data at a previous encrypting stage, said encrypting stage data at said

current encrypting stage indicating an encrypting state at said current encrypting stage (column 2 line 42 – column 3 line 51, column 5 lines 1-67);

(c) changing said encrypting operation to said text at said current encrypting stage when it is determined that said encrypting operation to said text at said current encrypting stage should be changed (Figure 2, Figure 4, column 2 lines 27-65, column 3 lines 12-51, column 5 lines 1-50);

(d) carrying out said encrypting operation to said text using first intermediate data at current encrypting stage of said encrypting operation (Figure 2, column 2 lines 27-65, column 5 lines 1-37, column 6 lines 1-65);

(e) executing said steps (b) to (d) for each of a plurality of encrypting stages of said encrypting operation to said text in response to said encrypt instruction to produce a ciphertext (Figure 2, column 2 lines 27-65, column 5 lines 1-37, column 6 lines 1-65);

(f) determining whether said decrypting operation to said text at a current decrypting stage should be changed, based on said decrypting stage data at a previous decrypting stage, said decrypting stage data at said current decrypting stage indicating an decrypting state at said current decrypting stage (Figure 12, column 9 lines 24-58);

(g) changing said decrypting operation to said text at said current decrypting stage when it is determined that said decrypting operation to said text at said current decrypting stage should be changed (Figure 12, column 9 lines 24-58);

(h) carrying out said decrypting operation to said text using second intermediate data at said current decrypting stage (Figure 12, column 9 lines 24-58); and

(i) executing said steps (f) to (h) for each of a plurality of decrypting stages of said encrypting operation to said text in response to said decrypt instruction to produce a plaintext (Figure 12, column 9 lines 24-58),

wherein step (b) determines whether said intermediate data at said next encrypting stage of said encrypting operation should be changed depending on at least a plurality of random numbers, based on said encrypting data at said current encrypting stage from said step (c) (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10),

wherein said encrypting stage data includes said intermediate data at said next encrypting stage (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10), and

wherein, in said step (c), said intermediate data at said next encrypting stage is changed a plurality of times depending on said plurality of random numbers, in order to cancel an influence of said plurality of random numbers on said encrypting operation (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10),

wherein step (f) determines whether said intermediate data at said next decrypting stage of said decrypting operation should be changed depending on at least a plurality of random numbers, based on said decrypting data at said current decrypting stage from said step (h) (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10),

wherein said decrypting stage data includes said intermediate data at said next encrypting stage (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10), and

wherein, in said step (f), said intermediate data at said next decrypting stage is changed a plurality of times depending on said plurality of random numbers, in order to

cancel an influence of said plurality of random numbers on said decrypting operation (column 2 lines 16 – 60, column 5 line 38 – column 6 line 10),

wherein said encrypting operation is carried about by:

i) dividing each n-bit word of the plaintext into an upper n bits and a lower n bits, n being an even integer value greater than or equal to 16,

ii) calculating a logical product of the upper n bits of the plaintext with at least one of said plurality of random numbers to obtain a first result, and

iii) calculating a logical product of the lower n bits of the plaintext with at least one of said plurality of random numbers to obtain a second result,

wherein, in obtaining the first result and the second result, a first subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with a first of said plurality of random numbers, a second subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with a second of said plurality of random numbers, and a third subset of the upper n bits and the lower n bits of the plaintext are exclusive-or'ed with both the first and second random numbers.

Examiner's Amendments to the Specification:

(Page 58, paragraph starting at line 9 and ending at line 17)

Referring to Fig. 7, the encrypting apparatus in the fourth embodiment is different from that of the first embodiment shown in Fig. 1 in the point that a recording medium 700 is

provided to store a program for the encrypting operation by the encrypting apparatus. The recording medium 700 may be a magnetic disk, a semiconductor memory, or a CD-ROM (Compact Disk-Read Only Memory).

(Page 59, paragraph starting at line 12 and ending at line 20)

Referring to Fig. 8, the encrypting apparatus in the fifth embodiment is different apparatus in the fifth embodiment is different from that of the first embodiment shown in Fig. 3 in point that a recording medium 800 is provided to store a program for the encrypting operation by the encrypting apparatus. The recording medium 800 may be a magnetic, a semiconductor memory, or a CD-ROM (Compact Disk-Read Only Memory).

(Page 60, paragraph starting line 15 and ending at line 23)

Referring to Fig. 9, the encrypting apparatus in the fifth embodiment is different from that of the first embodiment shown in Fig. 5 in the point that a recording medium 900 is provided to store a program for the encrypting operation by the encrypting apparatus. The recording medium 900 may be a magnetic disk, a semiconductor memory, or a CD-ROM (Compact Disk-Read Only Memory).

(Page 67, paragraph starting at line 2 and ending at line 10).

Referring to Fig. 13, the decrypting apparatus in the tenth embodiment shown in Fig. 10 in the point that a recording medium 1300 is provided to store a program for the decrypting process by the decrypting apparatus. The recording medium 1300 may be a magnetic disk, a semiconductor memory, or a CD-ROM (Compact Disk-Read Only Memory).

(Page 68, paragraph starting at line 6 and ending at line 14).

Referring to Fig. 14, the decrypting apparatus in the eleventh embodiment is different from that of the eight embodiment shown in Fig. 11 in the point that a recording medium 1400 is provided to store a program for the decrypting operation by the decrypting apparatus. The recording medium 1400 may be a magnetic disk, a semiconductor memory, or a CD-ROM (Compact Disk-Read Only Memory).

(Page 69, paragraph starting at line 10 and ending at line 18).

Referring to Fig. 15, the decrypting apparatus in the twelfth embodiment is different from that of the ninth embodiment shown in Fig. 12 in the point that a recording medium 1500 is provided to store a program for the decrypting operation by the decrypting apparatus. The recording medium 1500 may be a magnetic disk, a semiconductor memory, or a CD-ROM (Compact Disk-Read Only Memory).

(Page 78, paragraph starting at line 4 and ending at line 14).

Referring to Fig. 19, the encrypting and decrypting apparatus in the sixteenth embodiment is different from that of the thirteenth embodiment shown in Fig. 16 in the point that a recording medium 1900 is provided to store a program for the encrypting and decrypting operation by the encrypting and decrypting apparatus. The recording medium 1500 may be a magnetic disk, a semiconductor memory, or a CD-ROM (Compact Disk-Read Only Memory).

(Page 79, paragraph starting at line 12 and ending at line 22).

Referring to Fig. 20, the encrypting and decrypting apparatus in the seventeenth embodiment is different from that of the fourteenth embodiment shown in Fig. 17 in the point that a recording medium 2000 is provided to store a program for the encrypting and decrypting operation by the encrypting and decrypting apparatus. The recording medium 2000 may be a magnetic disk, a semiconductor memory, or a CD-ROM (Compact Disk-Read Only Memory).

(Page 80-80, paragraph starting on Page 80, line 20, and ending on Page 81, line 3).

Referring to Fig. 21, the encrypting and decrypting apparatus in the eighteenth embodiment is different from that of the fifteenth embodiment shown in Fig. 18 in the point that a recording medium 2100 is provided to store a program for the encrypting and decrypting operation by the encrypting and decrypting apparatus. The recording medium 2100 may be a magnetic disk, a semiconductor memory, or a CD-ROM (Compact Disk-Read Only Memory).

Allowable Subject Matter

1. Claims 1-63 were originally received for consideration. Through the course of examination new limitations, supported by the specification, were added to the independent claims, but no claims were added or cancelled. Claims 1-63 are allowed, subject to the amendment presented above to the claims and the specification.

2. The following is an examiner's statement of reasons for allowance:

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

The above mention claims are allowable over prior arts because the CPA (Cite Prior Art) of record fails to teach or render obvious the claim limitations in combination with

the specific added limitations added to the independent claims, claims 1,8,15,22,29,36,43,50, and 57, and subsequent dependent claims per the received Request for Continued Examination (RCE) received on April 7, 2005.

The CPA does not teach or suggest an apparatus and method of executing an encrypting and/or decrypting method which determines whether intermediate data at subsequent encrypting/decrypting stage should be changed based on stage data and a plurality of random numbers, wherein the encrypting operation includes dividing the plaintext into an upper and lower section, wherein the upper and lower section, and a plurality of random numbers are separately combined to produce two different results, further a first and second subset of the upper and lower bits, respectively, are exclusive-or'ed with a first and second plurality of random numbers, respectively, while a third subset of the upper and lower bits are exclusive-or'ed with both the first and second random numbers.

The present invention addresses the following drawbacks of prior art security mechanisms:

1) the lack of continued protection against cryptanalysis methods such as simple power analysis and differential power analysis.

Thus this invention provides a method for encrypting and/or decrypting plaintext, with a method that can change the encrypting operation and the intermediate data at the next stage depending on a plurality of random numbers and current stage data, and further, changes the intermediate data at a next encrypting stage a plurality of times

depending on a plurality of random numbers so that the influence of the plurality of random numbers are cancelled out.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KA
06/09/2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100